Post-Quanten-Kryptografie

Migration zu quantenresistenter Kryptografie

Tudor Soroceanu

Cybersicherheitstag am AISEC, 9.11.2023

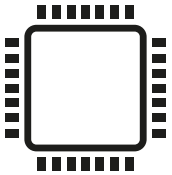
Quantencomputer

Fraunhofer AISEC

Quantum Computing

Klassische Bits vs. Quantenbits

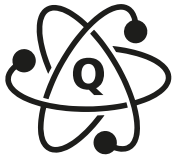
Bits

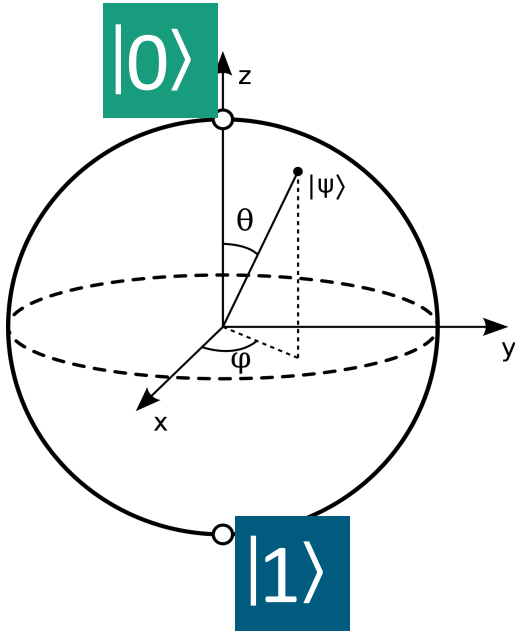


0

1

Qubits





Fraunhofer AISEC

Quantum Computing

Fortschritte der letzten Jahre

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

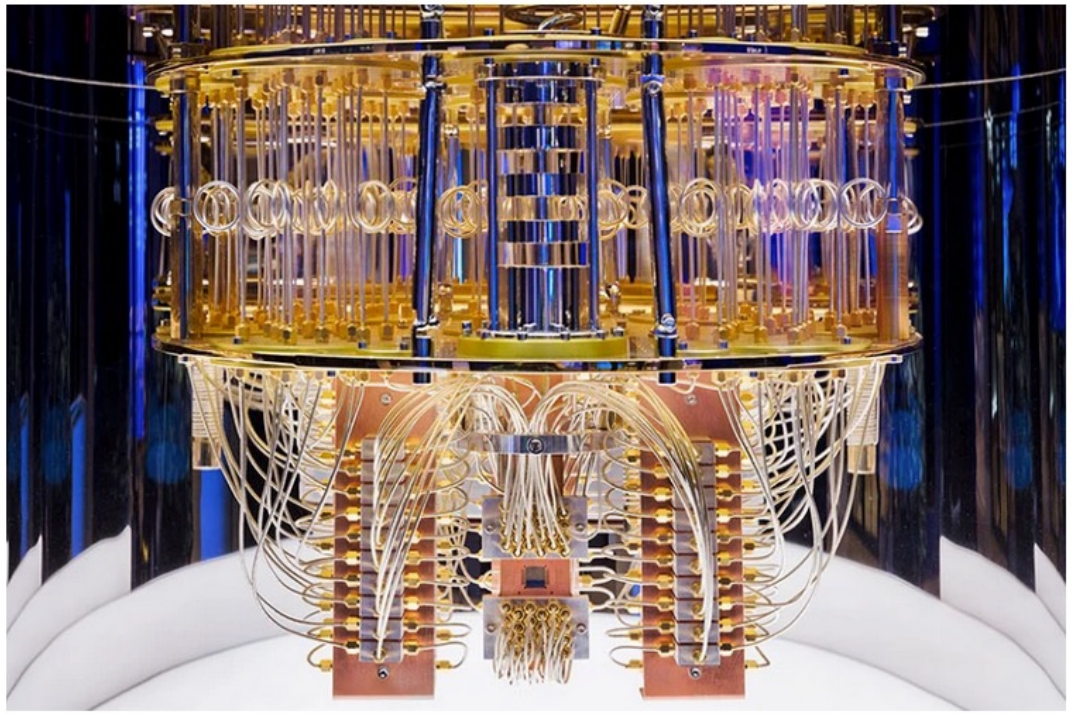
Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2–7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes

First quantum computer to pack 100 qubits enters crowded race

But IBM's latest quantum chip and its competitors face a long path towards making the machines useful.

Philip Ball



The innards of an IBM quantum computer show the tangle of cables used to control and read out its qubits. Credit: IBM

Fraunhofer AISEC

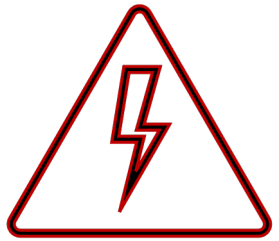
Quantencomputer und Kryptografie

Bedrohung von asymmetrischen Verfahren

Algorithmus von Shor
Bedroht Public-Key Verschlüsselung und digitale Signaturen.

Effizientes Faktorisieren

Effizientes Lösen des Diskreten Logarithmus



Angriff auf RSA

Angriff auf Diffie-Hellman, ECDH

Angriff auf (EC)DSA

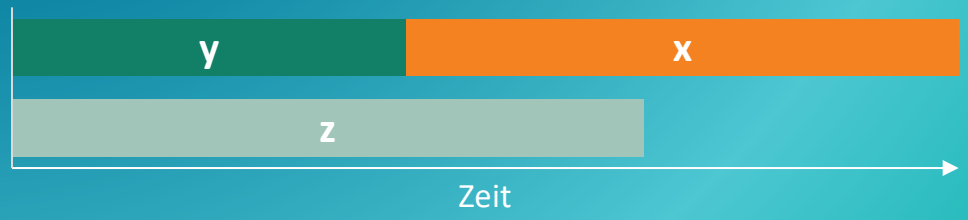
Shor, P.W. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994. https://doi.org/10.1109/SFCS.1994.365700.

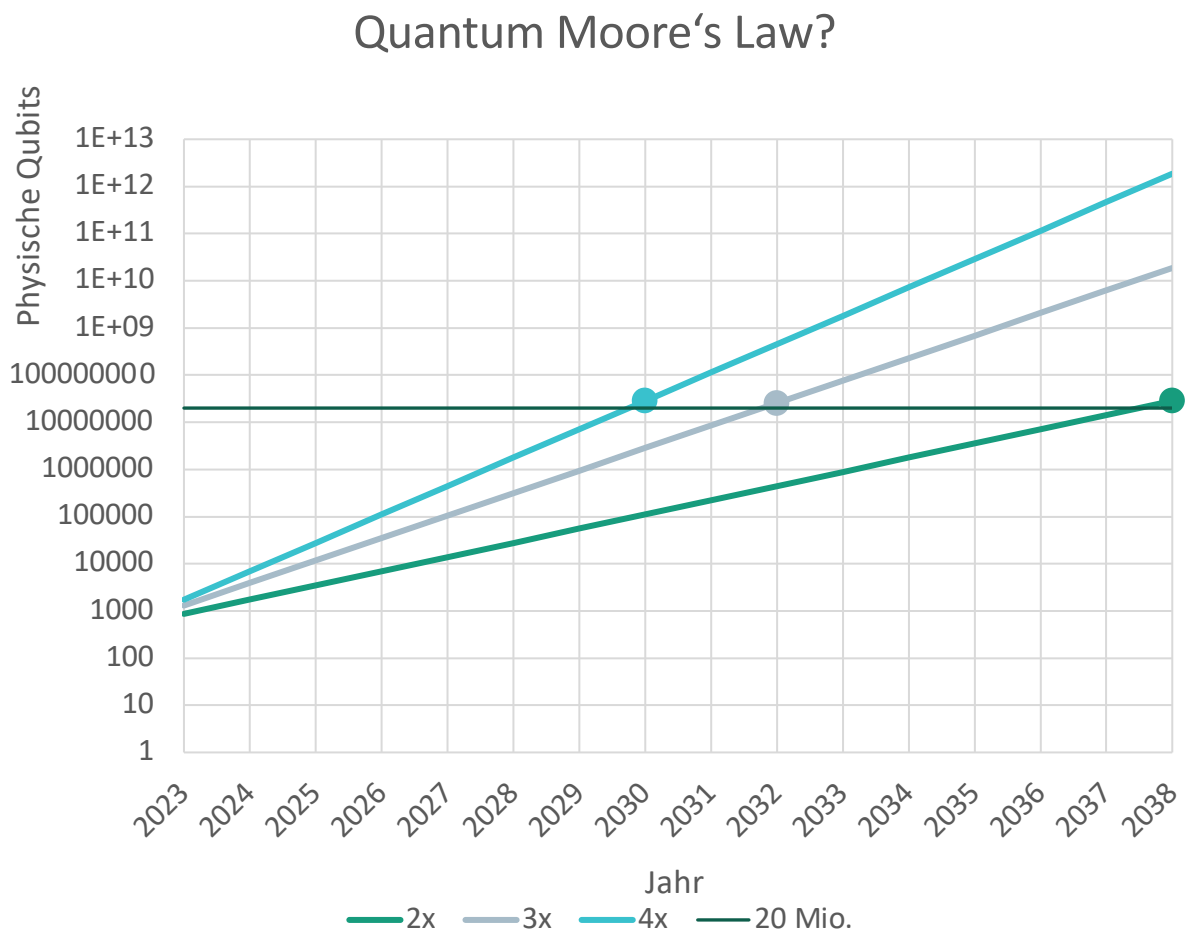
Quantencomputer
Forschung & Entwicklung

„Theorem“ von Michele Mosca

- x = *security shelf-life*
- y = *migration time*
- z = *collapse time*

Wenn x + y > z,
dann haben wir schon heute ein ernsthaftes Problem





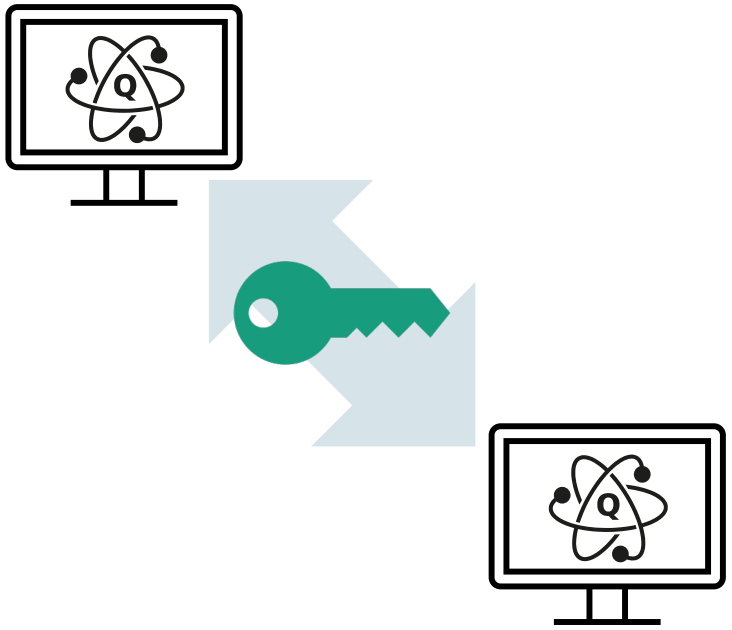
Fraunhofer AISEC

Post-Quanten-Kryptografie

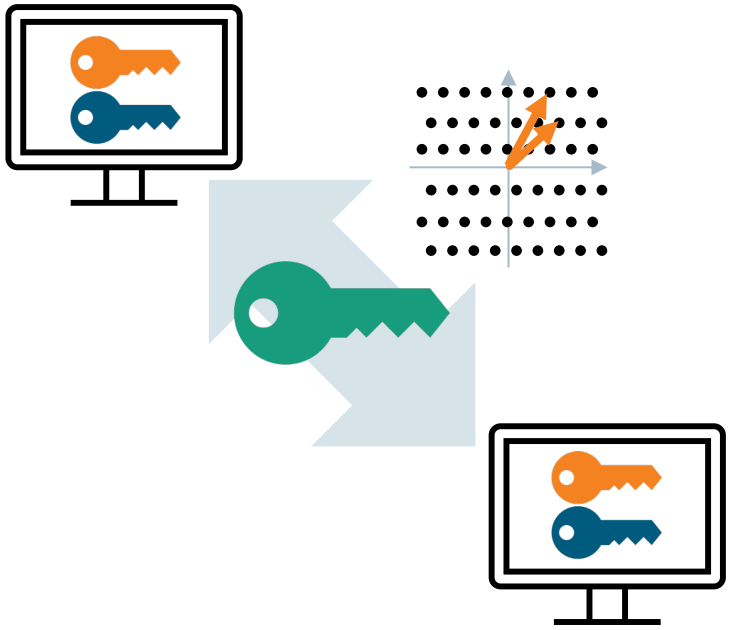
Schutz vor Kryptoanalyse durch Quantencomputer

Zwei verschiedene Ansätze

Quantum Key Distribution (QKD)

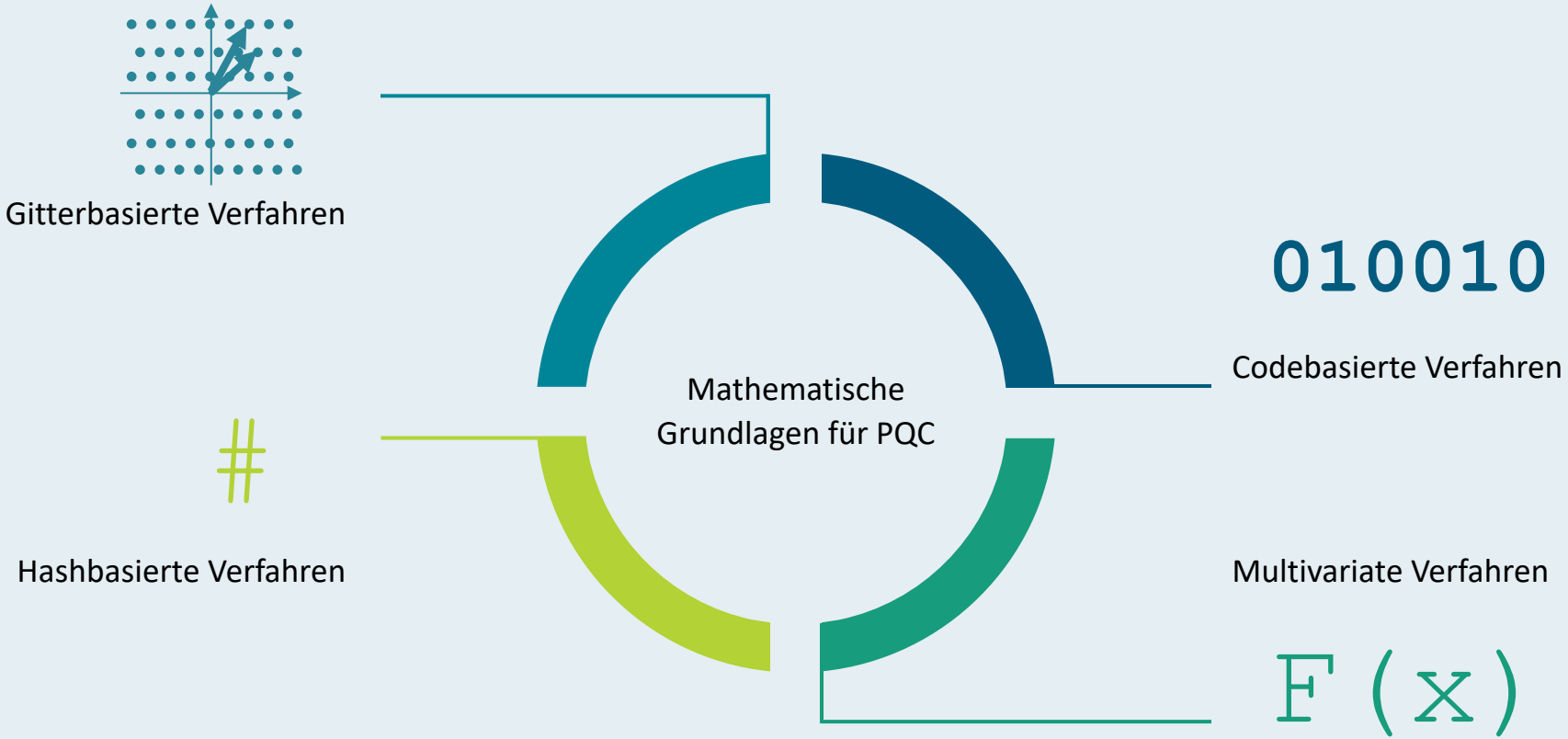


Post-Quanten-Kryptografie (PQC)



Post-Quanten-Kryptografie (PQC)

Herausforderungen für klassische Computer und Quantencomputer



Aktuelle Entwicklung von PQC-Standards

Standardisierung durch NIST und ISO

2016
NIST Call for Proposals
- 1. Runde mit 69 Einreichungen

2020
NIST PQC-Wettbewerb
- 3. Runde
- 7 Finalisten und 8 alternative Kandidaten

2022
NIST Standards
- KEM: Kyber
- Signaturen: Dilithium, Sphincs+, Falcon

2022+
ISO Standards
- Standardisierung von PQC-Verfahren

2023+
NIST CFP für Signaturen
- Suche nach Signaturen, die nicht auf Gittern basieren

PQC-Standards

Aktueller Stand der Standardisierung

Existierende Standards und Drafts für PQC-Algorithmen

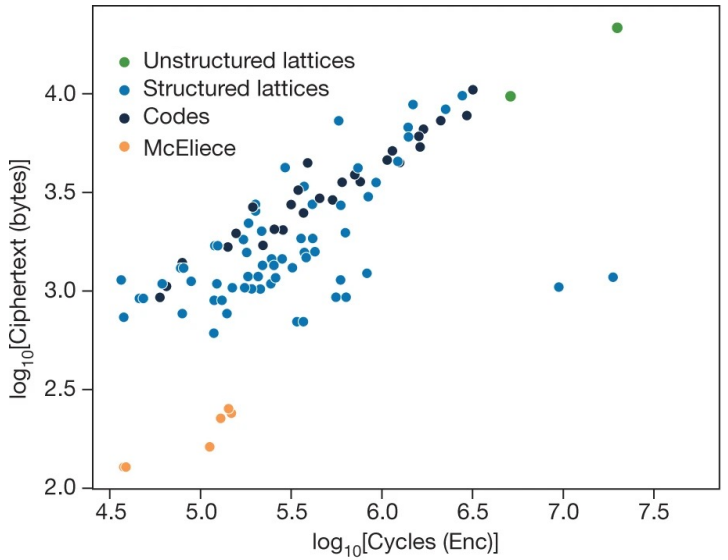
Algorithmus	Funktion	Math. Grundlage	Standard	Organisation
ML-KEM (Kyber)	KEM	Gitter	NIST Draft - FIPS 203 und Under Development - ISO/IEC 28033-2 Amd 2	NIST/ISO
FrodoKEM	KEM	Gitter	Under Development - ISO/IEC 28033-2 Amd 2	ISO
Classic McElice	KEM	Codes	Under Development - ISO/IEC 28033-2 Amd 2	ISO
ML-DSA (Dilithium)	Digital Signature	Gitter	NIST Draft - FIPS 204	NIST
SLH-DAS (Sphincs+)	Digital Signature	Hash	NIST Draft - FIPS 205	NIST
XMSS	Digital Signature	Hash	NIST SP 800-208	NIST
LMS	Digital Signature	Hash	NIST SP 800-208	NIST
FALCON	Digital Signature	Gitter	WIP	NIST

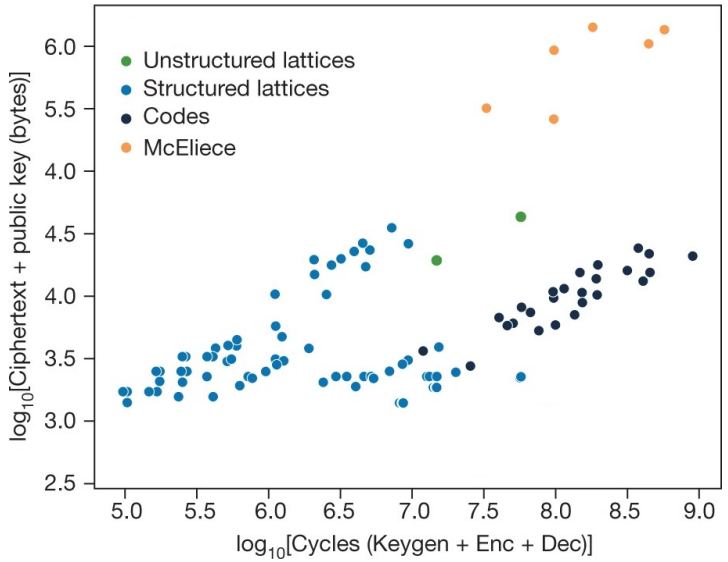
Migration zu Post-Quanten-Kryptografie

Migration zu PQC

Herausforderungen bei der Umsetzung

- PQC kein direkter Ersatz von klassischer Kryptografie
- Identifizieren betroffener Algorithmen
- Identifizieren von Kommunikationsprotokollen
- Umsetzung hybrider Mechanismen
- Auswahl standardisierter Verfahren
- Aktuelle Schlüsselgrößen und Hardware/Software-Limits
- Aktualisierbarkeit von Software
- Abhängigkeiten von Quellen der Schlüssel und Zertifikate
- Und viele weitere Challenges





Nature **605**, 237–243 (2022)

Angriffe auf PQC-Verfahren

An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

Abstract. We present an effic
singular Isogeny Diffie–Hellman
on Kani's "reducibility criterion
curves and strongly relies on t
Bob exchange during the protoc
morphism ring of the starting c
polynomial in the input size (he
of a small number of integers tha
The attack is particularly fast an
uses 2-isogenies and the starting
endomorphism of very small deg
tiation of SIDH that recently a
standardization effort for post-q
plementation breaks `SIKEp434`,
ten minutes on a single core.

Keywords: isogeny-based cryptogr

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens(✉)

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 h (one weekend) of computation time on a standard laptop.

Post-Quanten-Kryptografie: NIST in der Kritik wegen "dummen Rechenfehlers"

Die US-Normungsbehörde NIST hat sich beim Einschätzen der Stärke des Post-Quanten-Systems Kyber-512 völlig verrechnet. Der Experte Dan Bernstein ist besorgt.

Lesezeit: **5 Min.** In Pocket speichern 129

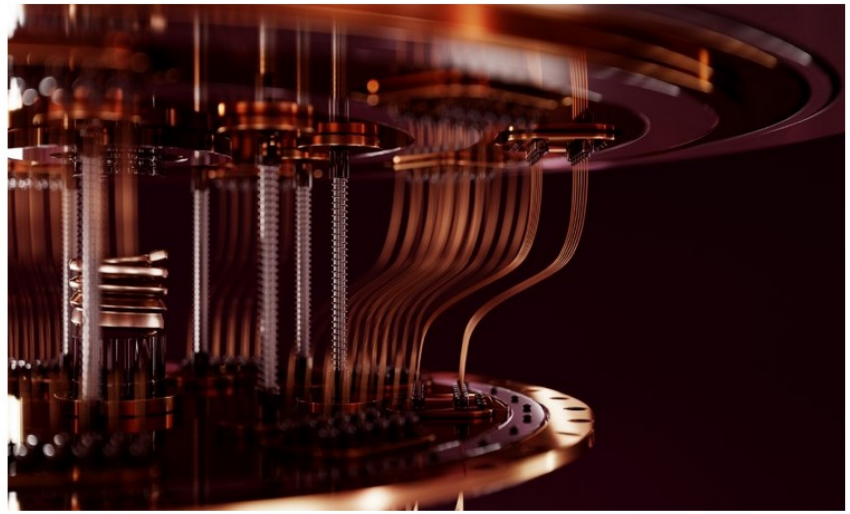
ki/Shutterstock.com)

Researcher Claims to Crack RSA-2048 With Quantum Computer

As Ed Gerck Readies Research Paper, Security Experts Say They Want to See Proof

Mathew J. Schwartz (euroinfosec) • November 1, 2023

Share Tweet Share Get Permission



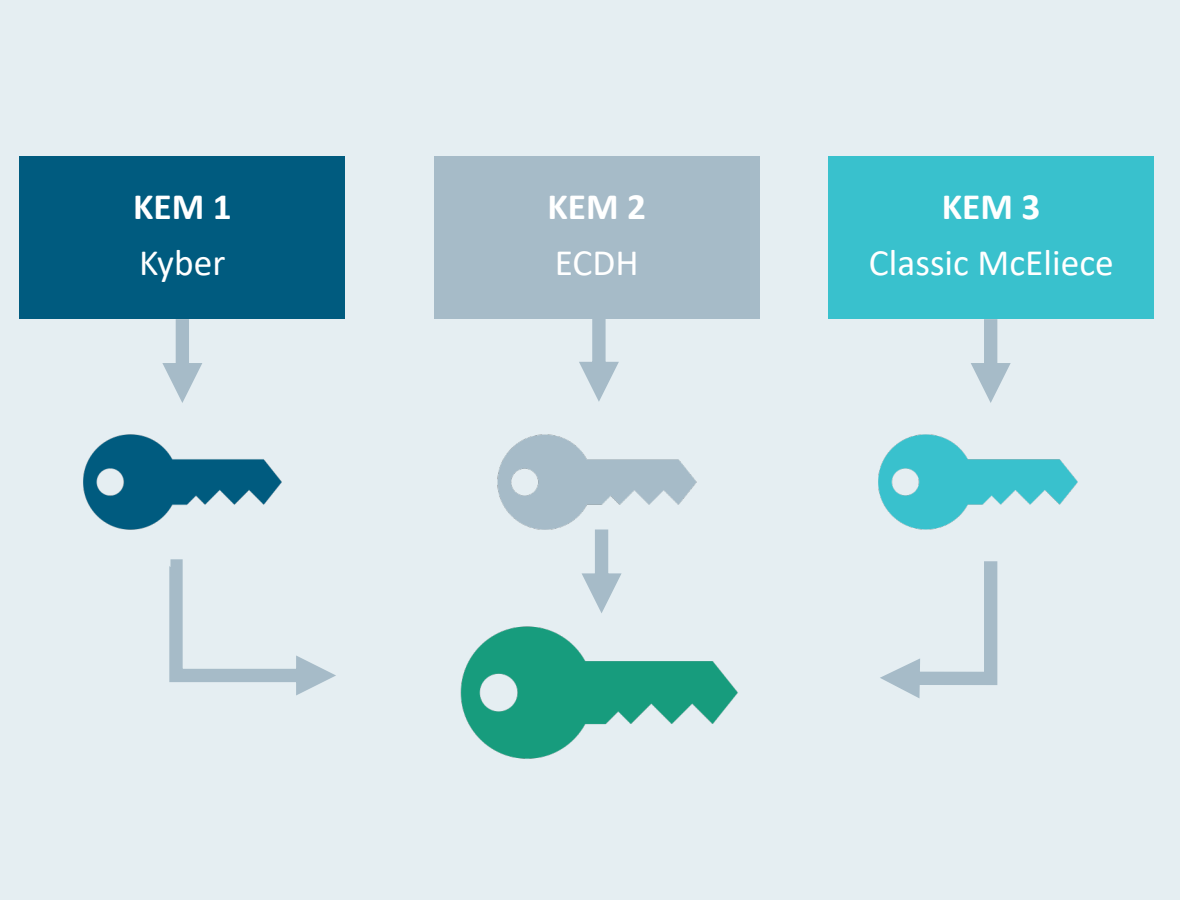
A 3-D render of a quantum computer. A scientist claims he cracked RSA-2048 encryption, but other scientists are skeptical. (Image: Shutterstock)

Fraunhofer AISEC

PQC + ECC

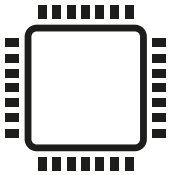
Hybride Verfahren als (Zwischen-)Lösung

- Kombination von klassischen und PQC-Algorithmen desselben Typs
- Ermöglicht den Umstieg auf PQC ohne aktuelle Sicherheitsgarantien zu verlieren
- Kombination bleibt sicher, auch wenn einzelne Verfahren gebrochen werden
- Achtlose Implementierung von hybriden Verfahren kann zusätzliche Angriffe ermöglichen



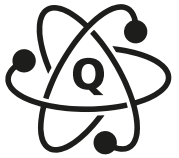
PQC@AISEC

Forschungstätigkeiten



Klassische Kryptoanalyse und Sicherheitsevaluierung

- Analyse von PQC-Verfahren, z.B.
  - Formale Verifikation
  - Seitenkanalanalyse
- Migrationsstrategien
- Sichere Implementierung von PQC



Kryptoanalyse mit Hilfe von Quantencomputern

Wie können Quantencomputer verwendet werden,

- um PQC-Verfahren zu brechen?
- um symmetrische Kryptografie zu brechen?

Kompetenzzentrum Post-Quanten-Kryptografie

Bündelung von PQC-Expertise am AISEC

Analyse von PQC-Implementierungen

https://www.aisec.fraunhofer.de/de/das-institut/kompetenzzentrum-post-quanten-kryptografie.html

Unterstützung bei Migration

Informationen zu PQC-Projekten

Jährlich stattfindender PQC-Workshop

Material zu branchentypischen Eigenheiten

Darstellung von wissenschaftlichem Fortschritt inklusive Folgenabschätzung

Kontakt

Tudor Soroceanu, M.Sc.
Department Secure Systems Engineering
Tel. +49 89 3229986-241
tudor.soroceanu@aisec.fraunhofer.de

Fraunhofer AISEC
Breite Str. 12
14199 Berlin
www.aisec.fraunhofer.de

Vielen Dank für Ihre Aufmerksamkeit

Fraunhofer AISEC